Statement of Philip K. Reitinger

Director, Trustworthy Computing - DC
Microsoft Corporation

Testimony before the

Subcommittee on Oversight and Investigations
House Committee on Energy and Commerce
U.S. House of Representatives

Hearing on "Making the Internet Safe for Kids:
The Role of ISP's and Social Networking Sites"

June 27, 2006

Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee, my name is Philip Reitinger. I am the Director for Trustworthy Computing in Washington, D.C. for Microsoft Corporation. Thank you for the opportunity to appear before you today to underscore Microsoft's strong commitment to protecting children from online predators and inappropriate material, and the steps we have taken to increase online safety. Before joining Microsoft, I was a Deputy Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice, the Executive Director of the Department of Defense Cyber Crime Center, and the Chair of the G8 Subgroup on High-Tech Crime. For much of my career I have been concerned with criminal online threats, and the challenges posed in preventing, detecting, deterring, and investigating cybercrime.

Microsoft is deeply and broadly engaged in efforts to protect children from Internet predators and inappropriate online material. Our efforts are focused in three general areas: (1) partnering with law enforcement to identify online threats to children and enable law enforcement to investigate and prosecute those who abuse or exploit them through the online environment, (2) empowering families through technological advances in our products and services to educate and protect their children, and (3) partnering with citizens, other companies, organizations, and government to educate communities more broadly regarding the risks to children in online activity and ways to keep them safe. In brief, Microsoft works with our partners to prevent child exploitation online, and actively supports law enforcement efforts in the U.S. and around the world to prosecute and punish those responsible for these heinous crimes.

Partnering with Law Enforcement to Identify, Investigate and Prosecute Child Pornography and Exploitation

As a technology leader, Microsoft understands and embraces its obligation to partner with law enforcement to combat child pornography and exploitation. When criminals harm children, online or offline, they must be caught, prosecuted, and punished. Microsoft views its partnership with law enforcement as critical to its efforts to protect children. First, Microsoft operates its online services so as to detect and prevent child pornography and exploitation, and works with law enforcement in its investigation of criminal acts. Second, Microsoft provides law enforcement specialized technology to help uncover, prosecute and convict criminals, and training to enhance its capabilities.

Abuse Detection and Reporting: MSN uses a filtering tool to review images uploaded to MSN Spaces and MSN Groups. Images that the filtering tool flags as potential child pornography are reviewed and, if child pornography is apparent, an incident report is sent to the National Center for Missing and Exploited Children (the National Center), pursuant to the requirements of the 1990 Victims of Child Abuse Act (1990 Act). Microsoft also follows the sound practices of the United States Internet Service Provider Association (USISPA) in reporting the facts or circumstances of apparent child pornography to the National Center, including providing samples of the images uploaded. Upon receiving this report, the National Center notifies law enforcement as provided in the 1990 Act. MSN closes the site and preserves the entire site, account information and associated files in anticipation of legal process

Microsoft also maintains a customer/user complaint capability, to review reports of child pornography or exploitation. When the central abuse handling support center confirms an apparent incident of child pornography or exploitation, it takes down the offending site and reports the incident to the National Center using the procedures described above.

Responding to Law Enforcement Requests: Microsoft's reports to the National Center set in motion a process under which law enforcement will request that Microsoft provide evidence of the criminal acts reported. Law enforcement also seeks evidence of child exploitation from Microsoft based on information law enforcement receives from other sources. Microsoft's compliance managers are on duty 24 hours a day 7 days a week to respond to requests from law enforcement to preserve or disclose evidence regarding criminal violations. Our compliance officers also educate and train U.S. and foreign law enforcement in how to obtain evidence from Microsoft regarding those engaged in child exploitation or pornography, consistent with U.S. law and privacy protections. Training law enforcement allows for better evidentiary requests and expedites law enforcement's process flow in collecting evidence.

The Child Exploitation Tracking System (CETS): In addition to providing to law enforcement evidence of criminal acts involving contacts with children online, Microsoft has developed technology to assist law enforcement in detecting, prosecuting and convicting child predators. In 2003, in response to a request to Bill Gates from Toronto Police Officer Detective Sergeant Paul Gillespie, Microsoft began developing CETS, an innovative, open standards-based software tool that enables law enforcement to better gather and share evidence of online child exploitation over a secure system based on legal agreements in place. CETS permits investigators to easily import, organize, analyze, share and search information from the point of detection through the investigative phase to arrest and conviction. The CETS system has now been adopted by law enforcement agencies across Canada. It has been incredibly rewarding to hear from our law enforcement colleagues in

Canada that the CETS already has played a part in several investigations across geographical boundaries, creating links that have helped apprehend over 40 online predators and, most importantly, led to the rescue of children in countries around the world. Microsoft also is working closely with several other law enforcement agencies around the world to assist with additional deployments to build a truly global network. To date, Microsoft has committed over $5 million to create the system and to help international police adopt and implement it.

Additional Support for U.S. Law Enforcement: Microsoft also sponsors federal, state and local law enforcement forensic and technical training programs to assist officers in cybercrime and child protection investigations, and continues to explore new opportunities to provide additional training of law enforcement officials. Microsoft also works closely with state Attorneys General in Florida, Georgia, New York, South Carolina, Texas, Washington and other states across the U.S. to develop tools and training and to provide technical support to investigations and prosecutions for online child exploitation and other cybercrimes.

Support for Foreign Law Enforcement and Global Cooperation Efforts: The Internet is a global environment and child exploitation is, sadly, a global tragedy. Helping to assure the online safety of children demands that Microsoft work around the globe, and within the law, to help protect users from inappropriate content, whatever its origin, and to help police around the world lawfully to apprehend child exploiters wherever they may be. Our efforts here include developing and deploying CETS and additional activities described below.

Global Campaign Against Child Pornography: In April 2004, Microsoft, Interpol and the International Centre for Missing and Exploited Children (International Centre) jointly announced the launch of the International Centre's Global Campaign Against Child

Pornography. As part of this campaign, Microsoft has contributed $1.5M to develop and implement a global training program for law enforcement. The training – known as the Computer Facilitated Crimes Against Children seminars -- consists of a series of four-day conferences designed to educate law enforcement officers around the world on identifying and investigating online criminal conduct against children; how to interact with victims and prevent further abuses; key issues such as human rights, data protection, and compliance with national laws; and managing complex international investigations. As of June 2006, 1,490 law enforcement officers from 91 countries have been trained in 16 regional training sessions in Europe, Central and South America, South Africa, Europe, Asia, and the Middle East.

Roundtable Discussions on Children's Online Safety: In addition to the training with the International Centre, Microsoft has sponsored a series of roundtable discussions on Children's Online Safety issues in countries around the world. These dialogues have brought together law enforcement officials, policymakers, industry experts and community leaders to examine how to stop illegal and harmful Internet activities targeting minors and small children, and to share best practices and lessons learned. The roundtables typically include panels examining the scope of the problem of online child exploitation and address child online safety from both public and private sector perspectives.

Virtual Global Task Force (VGTF): Through the VGTF, Microsoft has partnered with U.K., Australian, and Canadian law enforcement officials to develop a police reporting and patrol website and other initiatives. Additionally, the MSN Online Safety and Security site features a link to the VGTF Web site allowing individuals to report potentially illegal content.

CAN-SPAM and Efforts to Eliminate Spam: Microsoft's ongoing efforts against spam help to make the Internet safer for children because spam often contains links, messages and images not appropriate for children. Microsoft and other leading IT companies have partnered with enforcement officials worldwide to bring successful actions against unlawful spam. In addition, in March 2004, Microsoft and three other large Internet service providers — America Online, Earthlink, and Yahoo — filed multiple complaints in federal courts in the United States against hundreds of defendants for violating the CAN-SPAM Act, an important law that originated in the House Energy and Commerce Committee. Likewise, in September 2004, Microsoft joined with Amazon.com to file several lawsuits against chronic spammers who had targeted consumers by spoofing domains and phishing for consumers' personal information. In total, Microsoft's efforts to enforce anti-spam laws have produced more than 190 legal actions worldwide – with enforcement efforts in Asia Pacific, Europe and the Middle East, and the United States – and have resulted in approximately $869 million in legal judgments against spammers.

Cybercrime and Digital Forensics Workshop: On April 19-22, 2005, Microsoft and the Asian Development Bank Institute co-hosted an International Workshop on Cybercrime and Digital Forensics in connection with the 11th UN Congress on Crime Prevention and Criminal Justice. The workshop, developed for cybercrime investigators from countries across the Asia Pacific region, included practical, hands-on training from Microsoft specialists on the latest techniques in combating a range of computer crimes, including child exploitation.

Council of Europe Convention on Cybercrime: Microsoft has joined partners in industry to encourage countries, including the United States, to adopt and ratify the Council of Europe Convention on Cybercrime (COE Convention). The COE Convention is a powerful international instrument on cybercrime and is increasingly viewed as the global standard for criminalization obligations and governmental cooperation in this area. The COE Convention provides an important baseline for effective international cybercrime enforcement by requiring signatories to adopt and update laws and procedures to address crime in the online environment, and by providing for mutual investigative assistance between signatories. Notably, the COE Convention requires signatory nations to adopt laws criminalizing the production and distribution of child pornography through a computer system.

Financial Coalition Against Child Pornography: In March 2006, Microsoft joined the National Center and the International Centre and 16 of the world's leading financial institutions and other Internet industry leaders to form the Financial Coalition Against Child Pornography. The Coalition provides a forum for members to collaborate on a multi-pronged strategy with the objectives of closing down funding for child pornographers and eradicating commercial child pornography by 2008.

Model Legislation Against Child Pornography: In April 2006, Microsoft joined the International Centre in announcing support for model legislation against child pornography, and pledged to help pursue enactment of such legislation worldwide.

Safe Computing Program: Microsoft Canada and the University of Toronto's Center for Innovation Law and Policy launched the "Safe Computing Program" in 2005 to help in the fight against online child sexual exploitation. Microsoft Canada provided funding to the Centre for research and worked with the Office of the Attorney General (Ontario) in developing new policies.

INHOPE: Through software donations and training, Microsoft also supports INHOPE, the International Association of Internet Hotlines. INHOPE is a European

Union-supported organization with 23 member hotlines in 21 countries that responds to reports of illegal content to make the Internet safer.

Providing Safety Technology and Tools to Families

While partnerships with law enforcement are a critical component of efforts to protect children, empowering families to manage risk is equally important. We at Microsoft are committed to arming parents and guardians with both information to educate their children about online risks and technological tools to reduce such risks.

We continue to invest heavily in technologies that make computing more secure and the Internet experience safer for everyone. Tools we develop are made available globally in localized versions to enhance online security throughout the world. Our security and Internet safety efforts are driven by our Trustworthy Computing Initiative, which launched in 2002 and initiated a company-wide, top-to-bottom commitment to enhance the security and privacy of online users. At its heart, Trustworthy Computing is a long-term effort to create a secure, private and reliable computing experience for everyone and to increase user confidence in information technologies. Trustworthy Computing includes: support for the development of strong laws addressing criminal online conduct; support for law enforcement training, investigations, coordination and prosecutions; and encouraging and helping customers to adopt security best practices.

To assist parents in promoting online safety, Microsoft offers, and is investing in further development of, a variety of family safety technologies and tools. These tools employ user-friendly interfaces to make it simpler to act safely online, to help protect their personal information, and to permit parents and guardians to make and enforce informed and specific choices and to access activity reports about the Internet site visits their children made and the content to which they were exposed. These tools include both features of our web services, such as MSN Spaces, and family safety tools in the operating system and available for free from Windows Live. These family safety tools help families customize both their PC and their Web-based protection.

MSN: MSN Spaces, for example, allows users to create their own weblog, or *blog*, and invite others to view photos and messages. MSN Spaces employs strong abuse prevention and detection processes. In addition to the filtering capabilities referenced above, upon signing on to MSN Spaces, the user is warned in the Terms of Use and Code of Content that illegal uses of the technology are prohibited. The Code of Conduct expressly and prominently prohibits uploading, posting, transit, transfer, dissemination or distribution or facilitation of any content, including text, images, data, sound or software that is intended to harm or exploit minors, is illegal or violates local or national laws, including child pornography. See http://spaces.msn.com/coc.aspx. Other MSN properties have similar terms of use.

MSN Spaces is also designed with safety and privacy in mind. MSN Spaces' social networking features are designed to support developing closed networks of friends, not building networks of tens of thousands of unknown people. To complement user education, MSN Spaces also includes a number of features designed to enhance safety. For example, use of MSN Spaces requires that users have a Microsoft Passport. Offensive terms filtering is employed at the user name/alias and sub-title level, and privacy and communications preference controls are included. MSN Spaces also provides safety information, and information about how to set viewing and contact permissions directly on the MSN Spaces site and during the set up process for a Space. We recommend that all users keep personally identifying information to themselves, exercise care when posting photos with personal details, and never meet an Internet contact in person alone. MSN Spaces' safety tips also include a link to the short cautionary film "Predator," which a 14-year old boy wrote, directed and filmed working with his local police department. http://staysafe.org/teens/student_spotlight/predator.html.

In addition, MSN9 Premium Parental Controls incorporate content-filtering technology and offer several features that are designed to help parents manage their children's use of the Internet, while helping to protect them online. MSN Search offers a SafeSearch feature to filter sexually explicit content, and MSN contains pages developed specifically for kids.

Windows Vista: Through parental controls in our soon-to-be-released, next-generation Windows Vista operating system, parents will be able to control games played on a PC; establish time limits for how long their children use the computer; set gaming, application, Instant Messaging and Web restrictions; and receive logging and activity reports on their children's PC use. These controls will be easy to use yet allow detailed control – web browsing, for example, can be filtered by the type of content found on a web page. Windows Vista, as an open platform, will also enable users to run their choice of family safety software, and we anticipate working with a number of partners to enhance the family safety of the Windows Vista computing experience.

Windows Live Family Safety Settings: A free web service which will be available this year through the Windows Live set of online services, Windows Live Family Safety Settings was built to put better filtering tools in the hands of parents and guardians. By making these tools available for free, Microsoft is leading the industry in providing additional steps to enable parents and guardians to protect kids. Windows Live Family Safety Settings will provide web content filtering, including filtering of chat and mail; customized allow and block lists; customized approve/disapprove contact lists for Windows Live Instant Messenger (IM), MSN Spaces and Windows Live Hotmail; a kids request line that allows a parent to unblock a website in real time; roaming access to settings and activity reports on the web; and guidance for parents and kids from third party experts like the American Academy of Pediatrics. Windows Live Family Safety Settings will roll out in phases beginning this summer.

Xbox 360 and Xbox Live: Xbox 360 provides Family Settings worldwide to permit age-appropriate offline and online entertainment. Parents can restrict the games and DVD movies the console will play (based on established ratings systems, such as ESRB in the U.S.), as well as whether or not their children may create an Xbox Live account to play and communicate with fellow gamers online. The console's Family Settings apply to all users, so any game whose content surpasses the threshold set by the parent will not play unless a parent enters a secret code they have created. The Xbox Live Family Settings can be customized for each child in the family, and each child's personalized restrictions apply when the he or she plays Xbox away from home. Xbox Live Family Settings enable parents to control which friends may be added to the child's list of online contacts; disclosure of the child's online status; allowable communication methods, for example, whether the child can communicate via voice, video, or text messages; whether the child's gamer profile may be viewed by others and whether the child may view others' profiles; and game content (user-created or purchased content). Default settings are provided for children 12 or younger and ages 13-17. . In addition, Microsoft's guiding principles prohibit the functionality of certain game content (e.g., Microsoft does not manufacture or license others to create"adults-only" or sexually explicit games to run on Xbox consoles, and unlicensed game disks simply will not run, regardless of their content). See http://www.xbox.com/en-

US/support/familysettings/20051118-entertainmentcitizenship.htm. These investments earned Xbox Live the WiredKid's Safe Gaming Award in both 2003 and 2005.

Additional Safety Information: Microsoft has a wide range of safety and security information available on the various company and product websites. Microsoft.com - www.microsoft.com/athome/security, as well as websites for MSN - http://safety.msn.com, and for Xbox - http://www.xbox.com/en-US/support/familysettings/default.htm, provide information about online risks, training materials and tools to prevent safety issues.

We recognize that parents cannot always watch over their child's shoulder when he or she is on the computer. These parental tools directly address child online exploitation and child safety by giving parents the ability to better understand what their children are doing online, to shape and direct a child's online experience, to help generate productive conversations with children about safe behavior, and to manage the child's use of the Internet and the personal computer. For example, the ability to block a specific website – or category of websites – enables parents to put web chat or social networking sites on hold until they are sure their children understand and follow safety rules.

Moving forward, we will continue to invest in family safety innovation to enhance the protection offerings for our customers of the MSN network, Xbox 360 and Xbox Live, and our new Windows Live services.

Partnerships to Educate Communities About Child Online Safety

In addition to educating parents, Microsoft works to educate communities across the country and the world about risks to children online and tools to reduce these risks. The following provides a sampling of our efforts in this area.

GetNetSafe: A coalition of technology companies, educational organizations, government and advocacy groups[1] have joined together to support a national tour to raise awareness of computer security and Internet safety. During the 2006 tour of 12 U.S. cities experts will visit school assemblies and parents' nights, local community and senior events, business luncheons and Internet fairs to provide the information and tools communities need to protect themselves and their children. The tour will visit Washington DC, Boston, Phoenix, Dallas, Chicago, Detroit, New York City, Philadelphia, Charlotte, Los Angeles, Seattle, and Orlando.

Stay Safe Online and GetNetWise: Microsoft is a member of the National Cyber Security Alliance (NCSA), which is a partnership between the private sector and the Department of Homeland Security and the Federal Trade Commission to promote safe computing and the October "National Cyber Security Awareness Month" activities. The NCSA website, www.staysafeonline.info, has helpful material and information and tips about how to promote a more safe online computing experience for children and parents. These materials are available for use by anyone in the public or private sector who wants to help educate consumers. Microsoft also provides similar and supporting information.

In addition, Microsoft and several other leading technology companies, including AOL and AT&T, launched GetNetWise (www.getnetwise.org) as an online industry resource for parents and childcare providers. GetNetWise educates parents about the potential risks to children on the Internet and offers parents suggestions on how to interact with children regarding these risks. Additionally, GetNetWise provides parents with

[1] The Get Net Safe project was created by 12 partners, including: the Federal Trade Commission, the Department of Commerce, AARP, the National Center for Missing and Exploited Children (NCMEC), the U.S. Chamber of Commerce, i-SAFE America, RSVP, Boys and Girls Clubs of America, GetNetWise/Internet Education Foundation, National Cyber Security Alliance (NCSA), Microsoft Corporation and Best-Buy/Geek Squad.

information on the wide variety of available technological tools that can help limit children's access to inappropriate content and communications on the Internet.

Get Safe Online: Microsoft also is a major sponsor of the U.K.'s recently-launched "Get Safe Online" Internet Security campaign. As part of that campaign, we worked with the VGTF and ChildNet International to create an educational program for children, teachers, and parents entitled "Getting to Know IT All." As part of this pilot program, 175 Microsoft employees have been volunteering as trainers in schools and community centers around the United Kingdom teaching thousands of young people how to stay safe online.

Conclusion

Microsoft is strongly committed to improving online security for children and all our customers throughout the world, and to supporting investigation, prosecution, and punishment of child exploiters and predators. Through close partnerships with law enforcement, government officials and NGO's around the world, as well as technological advancements and parental education, we continue to make strides in combating online threats to our children. Through these means, Microsoft and its partners are in the process of developing and implementing best practices for protecting children.

Of course, in a field as important, rapidly changing, and complex as this one, there is always room for improvement, and we welcome feedback. Just as criminals find new ways to harm children, the good guys must be equally agile, working closely together to evolve methods for tracking and capturing child predators. To achieve such agility, there must be a global commitment to well-organized collaboration among policymakers, law enforcement, the NGO community, and industry. We at Microsoft will continue to look for new and innovative ways to collaborate with law enforcement, government officials at all levels, and other key participants in the fight against child exploitation, pushing the boundaries through technology solutions, and user education.

Thank you for the opportunity to speak with the Committee about this important topic.